Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes

Clemens Sauerwein[1], Christian Sillaber[1], and Ruth Breu[1]

[1] University of Innsbruck, Department of Computer Science, Innsbruck, Austria
{clemens.sauerwein,christian.sillaber,ruth.breu}@uibk.ac.at

Abstract. Cyber threat intelligence is obtained in an unstructured and ad-hoc manner from publicly available cyber security information sources such as security expert blogs or mailing lists. Although these information sources are used by employees as input for critical information security and risk management processes, they often have not received any formal IT department approval or assessment which raises issues in analogy to phenomenon of shadow IT. Little is known about the actual value these cyber security information sources provide and how they complement information security and risk management processes. In this paper, we conduct a structured, in-depth analysis of shadow cyber threat intelligence and investigate how it is used in organizations. Our study revealed that many heterogeneous and overlapping cyber security information sources serve as input for information security and risk management processes and that the obtained shadow threat intelligence is shared internally in a largely unstructured and informal manner.

Keywords: Threat Intelligence Sharing, Shadow IT, Information Security Risk Management

1 Introduction

Recent high profile security incidents have shown that the spectrum of possible attacks steadily increases and that the time frame for organizations to react shrinks constantly [1]. The protection of critical infrastructures, active vulnerability management, a fast internal dissemination of cyber security information and security awareness trainings have become key activities in organizations [2, 3]. To augment well established controls, a trend to systematically exchange cyber security information between organizations and with academia can be observed [4-6].

To aid vulnerability management and to mitigate incidents, security experts, security operatives and risk managers increasingly rely on a variety of information sources to augment their daily activities [7]. A multitude of different sources can be found, ranging from publicly available cyber security information sources (e.g. vulnerability databases) to inter-organizational cyber threat intelligence sharing platforms [8].

Research is mostly focused on how to build cyber threat intelligence sharing platforms and how to best structure the exchange of intelligence [9-13]. In this context, cyber threat intelligence describes any security related artifact that security and risk managers rely on during their information security and risk management processes.

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Apart from these cyber threat intelligence sharing platforms, security stakeholders rely to a large extent on publicly available sources. In contrast to cyber threat intelligence sharing platforms, this information is available in unstructured form and mostly used by employees inside the organizational ecosystem without any formal approval or systematic support from the IT department. Hence, the usage of these public available sources resembles in its nature the phenomenon of shadow IT [14, 15]. Accordingly, we introduce the concept of shadow cyber threat intelligence. *Shadow cyber threat intelligence can be defined as cyber threat intelligence obtained from cyber security information sources which are used inside an organization without explicit organizational approval or support.* Previous research showed that shadow IT introduces several risks [14, 16]. Therefore, a comprehensive understanding of the unexplored phenomena of shadow cyber threat intelligence and its implications for research and practice are warranted.

However, to which extent stakeholders utilize shadow cyber threat intelligence remains unclear as no scientific analysis of its use in information security and risk management processes exists and to the best of our knowledge, no empirical research has been conducted yet. To address this gap, we seek to answer the following research questions: (1) *Which shadow cyber threat intelligence sources can be identified in practice?* (2) *What are their characteristics and how is shadow cyber threat intelligence used in information security and risk management processes?*

The goal of our research is therefore to provide a comprehensive analysis of shadow cyber threat intelligence and its use in information security and risk management processes. To achieve this goal, we conducted a case study with 11 experts in the field. We identified 30 (shadow) cyber threat intelligence sources used by security experts to obtain timely and relevant cyber security information and mapped them to organizational information security and risk management processes. We observed that shadow cyber threat intelligence is used as input across all information security and risk management process, except processes related to the security mission (i.e. the most high level security management process). Finally, we discuss its use and how it is distributed to other stakeholders within the organization.

The remainder of this paper is structured as follows: Section 2 discusses related work. Section 3 outlines the underlying research methodology carried out. Section 4 outlines the key findings. Section 5 discusses the results and their implications for research. Section 6 discusses limitations of the research at hand. Finally, Section 7 concludes the paper and provides outlook on future work.

2 Related Work

The phenomena of employees using hardware, software or other solutions inside an organizational ecosystem which have not been formally approved by the IT department and bypassing official solutions has been described in research as shadow IT [17]. In this context, Silic and Back conducted a study to identify the types, usage, values, and risks of shadow IT used in organizations [14]. Several studies have shown that shadow

IT is some sort of insider threat where an employee uses (mostly in good faith) non-approved IT, violating company policies [15, 18].

Since these public cyber security information sources provide an enormous amount of information in a (mostly) unstructured manner, the identification and extraction of valuable cyber threat intelligence is challenging and might even hamper an effective security and risk management process. While researchers primarily focus on the extraction of cyber threat intelligence from social media platforms (e.g. Twitter) [19, 20], limited attention has been paid to other information sources, such as mailing lists, newspapers or security experts' blogs.

Previous research in the field of information security investigated the phenomenon of shadow security, where conscious employees create a more fitting alternative to the policies and mechanisms created by the organization's official information security team [21]. In this context, Kirlappos et. al showed that shadow security should not be treated as problem but as an opportunity to identify gaps in current security policies from which security managers can learn [22]. The research on shadow security focuses on non-compliant behavior to policies and security mechanisms and mostly omits security intelligence artifacts.

To the best of our knowledge, no prior research has been conducted on the nature and use of shadow threat intelligence sources in the context of information security and risk management processes or related areas.

3 Research Methodology

We conducted a case study to investigate the phenomenon of shadow cyber threat intelligence and its use in practice. The case study combines different methodological approaches to improve the resulting quality: (1) We conducted an exploratory survey [23] where the participants were asked to fill out a questionnaire in order to identify shadow cyber threat intelligence sources. They were also asked to identify their use within their organization's processes according to the participants' experience and observations. (2) The participants were asked to associate the identified cyber threat intelligence sources to information security and risk management activities. Finally, (3) we conducted a focus group discussion [23] to discuss the survey results, clarify participants' statements and analyze the participants' mapping of cyber threat intelligence sources to information security and risk management processes. The research was carried out in June 2016 at a neutral premise in a German-speaking country.

3.1 Participants of the Case Study

Table [1] gives an overview of the 11 participants of the case study, their organizational roles, type and size of organization.

Table 1. Overview of study participants

ID	*Organizational Role*	*Type of Org.*	*# of Employees*
1	Head of SOC	Finance	> 1000
2	Security Analyst	Insurance	> 1000
3	CISO	Finance	> 1000
4	Security Analyst	Production	> 1000
5	Security Analyst	Government	> 1000
6	Risk Manager	Finance	> 1000
7	Security Analyst	IT	150 -1000
8	Security Analyst	Production	> 1000
9	Incident Response Team	Finance	> 1000
10	Did not disclose	-	-
11	Did not disclose	-	-

Two of the participants decided to not disclose any information. The majority of participants work directly in their security operations center (e.g. as a security analyst, incident response team member) while only three participants are members of the managerial level (e.g. chief information security officer). Moreover, the composition of branches of industry represents a mixture of finance, production and information technology. While all companies operate globally, one of them is a medium- (150-1000 employees) and eight of them are large-sized organizations with more than 1000 employees each.

3.2 Exploratory Survey

The first part of our case study involved an exploratory survey which was used to identify the most important sources of shadow threat intelligence [23]. A survey was chosen as it is a valuable tool to investigate a technique or process (i.e. use of shadow cyber threat intelligence) in real-world settings [24].

For the exploratory survey, the participants (see Table 1) were asked to answer a questionnaire about the three most relevant (publicly available) cyber threat intelligence sources in use or they consider for use in their organization. In doing so, they had to specify the following for each identified information source: (i) Name of the cyber threat intelligence source, (ii) type of source, (iii) description of provided cyber threat intelligence, (iv) how often they access the information source, (v) how often obtained information had led to actionable events in their respective organization, (vi) how they had had shared information or key findings with colleagues and (vii) with whom from their organization they had shared the obtained information.

3.3 Mapping Session

Based on the questionnaire results, we generated a list of the identified threat intelligence sources and asked the participants in a subsequent mapping study to map each of them to an information security and risk management process, based on [25]. The process model, as depicted in Figure 1 (center), was used for the mapping session, consisted of the following four sub-processes: (1) Definition of security mission, (2) risk management (including threat analysis and vulnerability analysis), (3) implementation of security architecture, and (4) intuition. The information security and risk management process was displayed on a blackboard during the mapping session and explained to the participants in order to reduce uncertainties. Participants received index cards with the cyber threat intelligence sources identified in the previous session and were asked to pin the index cards to the respective security process where it serves as input.

3.4 Focus Group Discussion

Finally, we conducted a focus group discussion where we discussed the identified cyber threat intelligence sources, their nature, how they are accessed and their mapping to information security and risk management processes. This focus group discussion was held at a neutral premise and lasted roughly two hours. In order to minimize potential limitations, we followed the guidelines described in [26]. The whole focus group discussion was audio recorded. After the workshops, qualitative summaries were produced from the recordings [27] in order to derive findings relevant to our research questions [28].

4 Results

In this section, the key findings from the analysis of the case study are presented.

4.1 Shadow Cyber Threat Intelligence Sources Used in Organizations

Our exploratory survey identified 30 cyber threat intelligence sources. This include 25 shadow cyber threat intelligence sources that are used in practice and 5 formally approved and managed non-shadow sources. This low overall number can be traced back to the fact that we asked the participants to state only the three most important cyber threat intelligence sources they either use or had considered at their organization. The majority of identified shadow cyber threat intelligence sources are mailing lists (34%). 15% are vulnerability databases, 12 % vendor advisories, 6% social media streams, 6% face-to-face meetings, 6% blogs and 6% are other sources (e.g. whitepapers, reports). The remaining 12% are cyber threat intelligence sharing platforms. Study participants stated that these platforms have been officially approved by their respective IT departments and organizations mainly rely on them to obtain indicators of compromise (e.g. malicious IP addresses).

The identified mailing lists mainly focus on cyber security news including news about vulnerabilities, potential exploits, patching information, discussions of cyber security experts on hot topics and indicators of compromise.

The identified vulnerability databases are all using the conventional Common Vulnerabilities and Exposure (CVE) naming schema which standardizes the description of information security vulnerability names and enables the tracing of vulnerabilities over their lifecycle . Moreover, these databases provide CVE dictionaries augmented with additional information, descriptions, corresponding vulnerability severity scores (e.g. Common Vulnerability Scoring System) and search engine functionalities.

Four study participants stated that they visit vendor websites on a regularly basis in order to stay informed about vendor specific advisories. According to them, these advisories contain information about vulnerabilities and patches.

Our study participants frequently rely on social media streams, blogs and face-to-face meetings. In doing so, they exchange and discuss emerging topics in cyber security and share their "cyber war stories" (one respondent).

The focus group discussion showed that there is often no systematic process in place to discuss and access new cyber threat intelligence sources. The needed information is obtained "ad-hoc" through unstructured Google searches or face-to face meetings. In addition, four participants stated that new information sources are found by members of the security operations center, "... if they have time to look for them". Every participant identifies their own information sources without any official approval and coordination with other team members. Consequently, shadow cyber threat intelligence sources remain hidden from other team members and they are used without traces.

4.2 Motivation for the Use of Shadow Threat Intelligence Sources

According to the interviewees, one of the main motivations for using shadow cyber threat intelligence is the timely acquisition of information to stay up-to-date about emerging topics on cyber security. Our case study showed that security experts in organizations primarily focus on the procurement of information regarding new emerging vulnerabilities, indicators of compromise and available patches. In this context, it is noteworthy that the study participants scarcely rely on information regarding threat actors or countermeasures apart from patching.

According to [29], the data quality dimension of timeliness plays an important role for cyber threat intelligence sharing in general as outdated cyber threat intelligence loses its relevance and value quickly. We investigated how frequently shadow cyber threat intelligence sources are accessed within organizations: Almost half of the (shadow) cyber threat intelligence sources are accessed on a daily basis (40%), or instantaneous (20%). 17% of the identified sources are accessed weekly, 7% are monthly, 3% quarterly, 3% are biyearly, 3% yearly and the remaining 7% were not classified.

In order to get a better understanding of how relevant and useful the obtained shadow cyber threat intelligence is, we asked the participants to quantify how often obtained information led to actionable events. In 56% of the self-reported cases, cyber threat intelligence always, in 27% sometimes, and in 7% rarely led to actionable events. Merely in 7% of the cases shadow cyber threat intelligence never led to actions and the remaining 3% were not classified by the interviewees.

4.3 Organizations‘ Internal Distribution of Shadow Cyber Threat Intelligence

After the shadow cyber threat intelligence source is accessed and valuable information is extracted, the next step is to internally disseminate it. It might provide valuable and actionable information to other stakeholders and allows them to put countermeasures in place and prevents that two or more persons within an organization act on overlapping intelligence, which is one of the risks of shadow IT [14].

Our exploratory survey showed that 45% of obtained cyber threat intelligence are distributed via email, 17% via ticket systems, 13% via face-to-face meetings, 11% via forums or chats, 7% via cyber threat intelligence sharing platforms and 7% via security incident event management systems. This result is surprising as it can be expected that a cyber threat intelligence sharing platform would be the first choice to internally distribute cyber threat intelligence. We can conclude that the majority of cyber threat intelligence is distributed over a plethora of unstructured, manual and informal information channels (e.g. face-to-face, forums).

The obtained shadow cyber threat intelligence is mainly shared with cyber security professionals (e.g. security analysts) or the whole security operations team. In 52% of the cases, obtained intelligence is shared with the members of the security operations center, in 11% of the cases with security analysts, in 8% of the cases with the IT service department, in 7% of the cases with the incident response team, in 7% of the cases with the IT forensic department in 2% of the cases with the project management and in 2% of the cases with the IT infrastructure department.

4.4 Shadow Cyber Threat Intelligence as Input for Information Security and Risk Management Processes

After the information is obtained by an organization’s stakeholder, the information serves as input for information security and risk management processes. Shadow cyber threat intelligence sources primarily impact information security risk management processes (60% of the identified sources). In this context, shadow cyber threat intelligence is consulted during vulnerability (30%) and threat analysis (30%) processes in an ad-hoc manner without following any formal process. 27% of the identified sources are used for the implementation of a security architecture (e.g. developing security processes or implementing countermeasures). The remaining 13% of sources are used to support intuitive security management activities. None of the identified cyber security information sources serve as input to the definition of the security mission.

5 Discussion of Results

Figure [1] summarizes the results of our case study. It maps the identified shadow cyber threat intelligence sources to information security and risk management processes and shows how their outputs are internally distributed with responsible stakeholder groups.

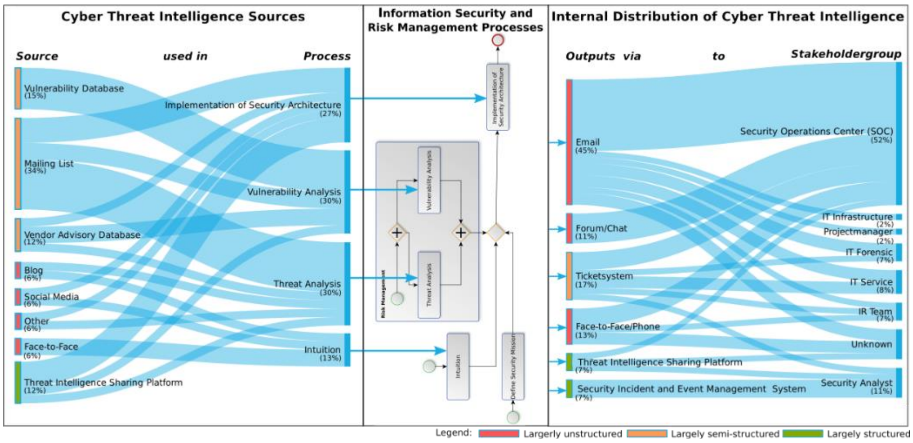
Cyber Threat Intelligence Sources
Source
used in
Process
Vulnerability Database (15%)
Mailing List (34%)
Vendor Advisory Database (12%)
Blog (6%)
Social Media (6%)
Other (6%)
Face-to-Face (6%)
Threat Intelligence Sharing Platform (12%)
Implementation of Security Architecture (27%)
Vulnerability Analysis (30%)
Threat Analysis (30%)
Intuition (13%)
Information Security and Risk Management Processes
Implementation of Security Architecture
Vulnerability Analysis
Threat Analysis
Risk Management
Intuition
Define Security Mission
Internal Distribution of Cyber Threat Intelligence
Outputs via
to
Stakeholdergroup
Email (45%)
Forum/Chat (11%)
Ticketsystem (17%)
Face-to-Face/Phone (13%)
Threat Intelligence Sharing Platform (7%)
Security Incident and Event Management System (7%)
Security Operations Center (SOC) (52%)
IT Infrastructure (2%)
Projectmanager (2%)
IT Forensic (7%)
IT Service (8%)
IR Team (7%)
Unknown
Security Analyst (11%)
Legend: 🟥 Largerly unstructured 🟧 Largely semi-structured 🟩 Largely structured

Figure 1. Overview of study results: Mapping of (shadow) cyber threat intelligence sources to information security and risk management processes (based on [25]) and an organization's internal distribution of the outputs

As discussed in Section 4, and depicted in Figure [1], mailing lists (34%), vulnerability databases (15%) and vendor advisories (12%) form the majority of shadow cyber threat intelligence sources accessed in practice. A closer analysis of the types of information obtained from these sources showed that diverse information on different abstraction levels are used. In this context, the heterogeneity of the obtained information ranges from technical indicators of compromise (e.g. hash values, IP addresses, domain names), to informal discussions between security experts about new emerging vulnerabilities or tactics, techniques and procedures carried out by threat actors. Moreover, shadow cyber threat intelligence is distributed over different channels (e.g. social media, mailing lists). Different vocabularies are used, and content is available in a mostly unstructured form.

Consequently, the automatic processing of shadow cyber threat intelligence is infeasible, which increases the complexity of the collection and processing of the obtained information as most steps have to be conducted manually. This leads to the observation that mostly the low hanging fruits, such as IP addresses, hash values of suspicious files, domain names or CVEs are used as input for information security and risk management processes. Moreover, this has been confirmed by the majority of study participants in so far as they stated, that they are mainly interested in indicators of compromise as they don't have the resources, time and software solutions required to analyze more complex cyber threat intelligence.

Our case study showed that shadow cyber threat intelligence serves as input for information security and risk management processes in organizations and represents an additional information source in addition to traditional ones, such as log files or penetration testing results. Moreover, the participants stated that one of the core motivations to rely on shared cyber threat intelligence is the timely acquisition and processing of security related information. Moreover, the case study showed that shadow cyber threat intelligence sources are accessed in 60% of the cases on a daily (including instantaneous) basis and more than 50% of used sources provided intelligence that lead to actionable events. These facts clarify the value and importance of shadow cyber threat intelligence for organizations.

Our research confirmed that the reliance on shadow threat intelligence can undermine the officially approved information security and risk management process. As a result, intelligence available to decision makers might be incomplete, duplicate already existing information, or faulty which would lead to undesired effects, e.g. information security experts might be fooled and miss potential threats to their information systems. In addition, unapproved shadow cyber threat intelligence sources might become more important than official cyber security information sources in organizations, which might constitute a single point of failure, hidden to senior cyber security stakeholders. As the majority of shadow threat intelligence is obtained and distributed through conventional information channels, as depicted in Figure 1, it is hard to implement controls or take actions to avoid the usage of shadow cyber threat intelligence.

Our research revealed that shadow cyber threat intelligence endangers structured organizational information flows. The majority of study participants mentioned that everybody relies on their own information sources and collects the needed cyber threat intelligence without consulting other employees. Unfortunately, this informal and inconsistent approach might be traced back to a lack of a formal workflow to collect and distribute cyber threat intelligence in organizations. Accordingly, this might lead to wasted resources as the information must be distributed and reconsolidated by other employees. This loss of efficiency is problematic as time plays a crucial role in information security and risk management processes. For example, according to one participant, the earlier an identified threat is communicated to responsible persons within the security operations center, the sooner countermeasures can be implemented. A closer look on how the study participants share the obtained shadow cyber threat intelligence in their organization, showed that they primarily rely on email or face-to-face exchanges. This might lead to information loss and a lack of traceability. The focus group discussion showed that a more formal approach such as using a threat intelligence sharing platform could be a suitable solution to address these problems. However, our investigations showed that only 7% of the organizations participating in our study use a cyber threat intelligence sharing platform to distribute the obtained shadow cyber threat intelligence.

Finally, our case study showed that the majority (57%) of shadow cyber threat intelligence sources serve as input for risk management processes. This is not surprising as processes such as vulnerability analysis or threat analysis primarily focus on the collection of recent information regarding vulnerabilities, threats and threat agents. Moreover, the interviewees stated that the obtained cyber threat intelligence triggers proactive information security and risk management processes. For example, six participants stated that they evaluate if their system is at risk through checking the internal documentation, architecture and log files against the received cyber threat intelligence.

6 Limitations

The research at hand might be limited by certain threats to validity that have to be acknowledged. In order to minimize them, we attempt to triangulate our findings through an exploratory survey followed by a two-stage focus group discussion with information security experts. Limitations that have to be acknowledged and accounted for are: (i) limited generalizability of the results, (ii) selection bias when selecting the participants of the case study (including the exploratory survey, mapping session and focus group discussion), (iii) influences of moderators during focus group discussions, (iv) off-topic discussions, (v) language barriers, (vi) incomplete or biased list of identified shadow cyber threat intelligence sources, (vii) biased mapping of shadow threat intelligence sources to information security and risk management processes and (viii) biased description of shadow cyber threat intelligence sources.

Limitation (i) results from a small sample size of participants and identified (shadow) cyber threat intelligence sources. This was consciously accepted as the focus of the case study was to qualitatively investigate the phenomenon of shadow cyber threat intelligence. Limitations (ii) to (v) primarily result from conducting an exploratory survey and focus group discussion research [30]. They might be counteracted by following the suggestions of Vogt et al. [26]. By following them, (ii) participants of the case study were asked to participate voluntarily at a neutral premise, (iii) moderators tried to keep in the background as much as possible, (iv) moderators refocused the discussion as soon as it got off track and eliminated any uncertainties by answering questions raised, and (v) the exploratory survey and focus group discussions were held in English as a common language. To counteract (vi), the participants were asked to fill out a questionnaire for the three most relevant shadow cyber threat intelligence sources without exchange with other participants. Secondly, to overcome (vii), the participants had to map the identified intelligence sources to information security and risk management processes (based on [25]) on their own without any discussion. Finally, to counteract limitation (vii), the participants had to describe the nature of their identified cyber threat intelligence sources, which served as input to guide the focus group discussion.

7 Conclusion

In this paper, we investigate the phenomenon of shadow cyber threat intelligence, i.e. the unstructured and unapproved use of cyber threat intelligence and its dissemination in organization in a case study with 11 security experts from medium to large-sized organizations. The case study showed that a multitude of different shadow cyber threat intelligence sources are used as input for information security and risk management processes. Moreover, we figured out that the use of shadow cyber threat intelligence might bypass security and risk management review processes or formal approval structures (or at least reduce the amount of information available in tangible form). This goes hand-in-hand with a loss of knowledge as shadow cyber threat intelligence could be lost in email message chains, undocumented face-to-face meetings or social media messages. During audits or forensic postmortem analysis, attempting to reconstruct whether security and risk management processes have been implemented properly, the hard-to-trace nature of shadow cyber threat intelligence could lead to a skewed or incomplete picture of the process. Future work will focus on empirical research on the phenomenon of shadow cyber threat intelligence, associated risks and how to extract its value in a way compatible with organizational requirements.

References

1. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences 80, 973-993 (2014)
2. Soomro, Z.A., Shah, M.H., Ahmed, J.: Information security management needs more holistic approach: A literature review. International Journal of Information Management 36, 215-225 (2016)
3. Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. Mis Quarterly 757-778 (2010)
4. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F.: Current challenges in information security risk management. Information Management & Computer Security 22, 410-430 (2014)
5. Fransen, F., Smulders, A., Kerkdijk, R.: Cyber security information exchange to gain insight into the effects of cyber threats and incidents. e & i Elektrotechnik und Informationstechnik 132, 106-112 (2015)
6. Skopik, F., Settanni, G., Fiedler, R.: A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security 60, 154-176 (2016)
7. Shackleford, D.: Who's Using Cyberthreat Intelligence and How? SANS Institute. Retrieved February 23, 2016 (2015)
8. Sauerwein, C., Sillaber, C., Mussmann, A., Breu, R.: Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In: Proccedings of the Wirtschaftsinformatik (WI) (2017)
9. Dandurand, L., Serrano, O.S.: Towards improved cyber security information sharing. In: Cyber Conflict (CyCon), 2013 5th International Conference on, pp. 1-16. IEEE, (2013)
10. Serrano, O., Dandurand, L., Brown, S.: On the design of a cyber security data sharing system. In: Proceedings of the 1st ACM Workshop on Information Sharing & Collaborative Security, pp. 61-69. ACM, (2014)
11. Brown, S., Gommers, J., Serrano, O.: From cyber security information sharing to threat management. In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, pp. 43-49. ACM, (2015)
12. Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C.: Guide to cyber threat information sharing. NIST Special Publication 800, 150 (2016)
13. Kampanakis, P.: Security automation and threat information-sharing options. IEEE Security & Privacy 12, 42-51 (2014)
14. Silic, M., Back, A.: Shadow IT–A view from behind the curtain. Computers & Security 45, 274-283 (2014)

15. Györy, A.A.B., Cleven, A., Uebernickel, F., Brenner, W.: Exploring the shadows: IT governance approaches to user-driven innovation. In: Proccedings of the European Conference on Information Systems (ECIS) (2012)

16. Strong, D.M., Volkoff, O.: A roadmap for enterprise system implementation. Computer 37, 22-29 (2004)

17. Behrens, S., Sedera, W.: Why do shadow systems exist after an ERP implementation? Lessons from a case study. In: Proceedings of the Pacific Asia Confernece on Information Systems (PACIS) (2004)

18. Warkentin, M., Willison, R.: Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems 18, 101-105 (2009)

19. Cui, B., Moskal, S., Du, H., Yang, S.J.: Who shall we follow in twitter for cyber vulnerability? In: SBP, pp. 394-402. Springer, (2013)

20. Sabottke, C., Suciu, O., Dumitras, T.: Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits. In: USENIX Security Symposium, pp. 1041-1056. (2015)

21. Kirlappos, I., Parkin, S., Sasse, M.A.: Learning from “Shadow Security”: Why understanding non-compliance provides the basis for effective security. In: (Proceedings) Workshop on Usable Security (2014)

22. Kirlappos, I., Parkin, S., Sasse, M.A.: Shadow security as a tool for the learning organization. ACM SIGCAS Computers and Society 45, 29-37 (2015)

23. Babbie, E.R.: Survey research methods. Wadsworth (1973)

24. Pfleeger, S.L.: Experimental design and analysis in software engineering. Annals of Software Engineering 1, 219-253 (1995)

25. Pettigrew, J., Ryan, J.: Making successful security decisions: a qualitative evaluation. IEEE Security & Privacy 10, 60-68 (2012)

26. Vogt, D.S., King, D.W., King, L.A.: Focus groups in psychological assessment: enhancing content validity by consulting members of the target population. Psychological assessment 16, 231 (2004)

27. Mayring, P., Gläser-Zikuda, M.: Die Praxis der Qualitativen Inhaltsanalyse. Beltz Weinheim (2008)

28. Campbell, J.L., Quincy, C., Osserman, J., Pedersen, O.K.: Coding in-depth semistructured interviews: Problems of unitization and intercoder reliability and agreement. Sociological Methods & Research 42, 294-320 (2013)

29. Sillaber, C., Sauerwein, C., Mussmann, A., Breu, R.: Data quality challenges and future research directions in threat intelligence sharing practice. In: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 65-70. ACM, (2016)

30. Louise Barriball, K., While, A.: Collecting Data using a semi-structured interview: a discussion paper. Journal of advanced nursing 19, 328-335 (1994)